PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-267957
(43)Date of publication of application : 29.09.2000

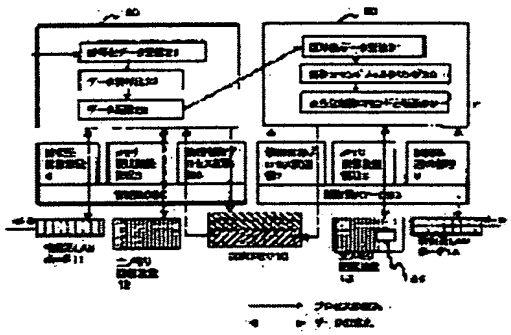
(51)Int.Cl. G06F 13/00
G06F 9/46
H04L 12/46
H04L 12/28

(21)Application number : 11-069575
(22)Date of filing : 16.03.1999

(71)Applicant : HITACHI LTD
(72)Inventor : FURUYA MASATOSHI
SEKOZAWA TERUJI
KATO HIROMITSU

(54) FIRE WALL FOR CONTROL SYSTEM

(57)Abstract:
PROBLEM TO BE SOLVED: To obtain the fire wall which has a function of transferring only commands useful to the control system to the control system by filtering commands obtained by inter-process communication and communicating allowed commands to a monitor and control computer.
SOLUTION: The fire wall for control system is mounted on a computer where a general purpose operating system (G-OS) and a dedicated real-time operating system (RT-OS) coexist. Processes on the G-OS and RT-OS are enabled to communicate with each other. At this time, an information system process 20 on the G-OS receives and decodes coded data and passes the decoded data to a control system process 30 on the RT-OS. Then the control system process 30 extracts control commands extracted from the data and transfers only passable commands to a monitor computer, etc., on a control system LAN by referring to a command filtering table.



CU

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2000－267957
（P2000－267957A）
(43)公開日　平成12年９月29日(2000.9.29)

(51)Int.Cl.[7]	識別記号	ＦＩ		テーマコード（参考）
Ｇ０６Ｆ　13/00	３５１	Ｇ０６Ｆ　13/00	３５１Ｚ	５Ｂ０８９
9/46	３６０	9/46	３６０Ｆ	５Ｂ０９８
Ｈ０４Ｌ　12/46		Ｈ０４Ｌ　11/00	３１０Ｃ	５Ｋ０３３
12/28				

審査請求　未請求　請求項の数５　ＯＬ　（全 18 頁）

(21)出願番号　特願平11－69575

(22)出願日　平成11年３月16日(1999.3.16)

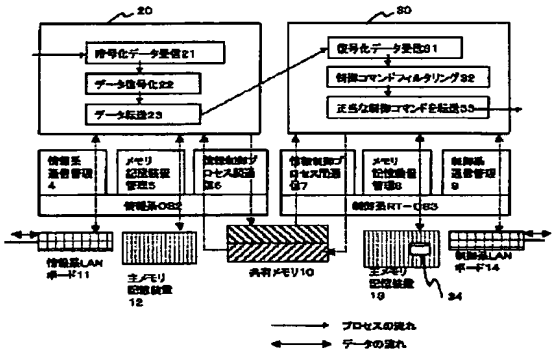
(71)出願人　000005108
株式会社日立製作所
東京都千代田区神田駿河台四丁目６番地
(72)発明者　古谷　雅年
神奈川県川崎市麻生区王禅寺1099番地　株式会社日立製作所システム開発研究所内
(72)発明者　瀬古沢　照治
神奈川県川崎市麻生区王禅寺1099番地　株式会社日立製作所システム開発研究所内
(74)代理人　100068504
弁理士　小川　勝男

最終頁に続く

(54)【発明の名称】　制御系用ファイアウォール

(57)【要約】
【課題】制御系ＬＡＮと情報系ＬＡＮとの接点において、悪意、または、無意識による制御系への不正介入、トラフィック妨害を防ぐための制御系用ファイアウォールを提供する。
【解決手段】情報系プロセスで、暗号化データを受信し、そのデータを復号化し、復号化したデータを制御系プロセスに渡し、データから制御コマンドを抽出し、コマンドフィルタリングテーブルを参照して、「通過」できる制御コマンドだけフィルタリングして、制御系ＬＡＮ上の監視制御コンピュータなどに転送する。また、制御系プロセスで、監視データを受信し、プロセス間通信で情報系プロセスに渡し、さらに、情報系ＬＡＮ上の端末やデータベースサーバに転送する。

図1



1

【特許請求の範囲】

【請求項１】制御機器を制御したり、計測機器からデータを収集したりする監視制御用コンピュータが接続されている制御系ネットワークに接続する制御系ＬＡＮボードと、情報端末や情報サーバが接続されている情報系ネットワークに情報系ＬＡＮボードとを搭載し、制御系用リアルタイムオペレーティングシステムと情報系用オペレーティングシステムとが動作し、制御系用通信プロトコルで通信する手段と情報系用通信プロトコルで通信する手段とを有し、制御系用リアルタイムオペレーティングシステム上で動作するプロセスと情報系用オペレーティングシステム上で動作するプロセスとがプロセス間通信する手段を有するコンピュータであって、情報系用オペレーティングシステム上では、情報系ネットワークから送信された暗号化コマンドを復号化する手段と、復号化したコマンドを制御系用リアルタイムオペレーティングシステム上で動作するプロセスにプロセス間通信する手段とを有し、制御系用リアルタイムオペレーティングシステム上では、プロセス間通信によって入手したコマンドをフィルタリングする手段と、フィルタリング手段によって許可されたコマンドを前記監視制御用コンピュータに通信する手段とを有していることを特徴とする制御系用ファイアウォール。

【請求項２】請求項１記載の制御用ファイアウォールであって、制御系用リアルタイムオペレーティングシステム上では、制御可能なコマンド情報、または、監視データを制御系ネットワークから受信し、受信した内容に基づいてコマンドをフィルタリングするルールを変更する手段を有していることを特徴とする制御系用ファイアウォール。

【請求項３】請求項１記載の制御系用ファイアウォールであって、コマンドフィルタリング手段のためのフィルタリングルールを記憶する記憶装置は、制御系用リアルタイムオペレーティングシステム上で動作するプロセスからのみ読み書き可能なことを特徴とする制御系用ファイアウォール。

【請求項４】請求項１記載の制御系用ファイアウォールであって、情報系用オペレーティングシステム上では、コマンドを送信したユーザが正当な権利をもつかを認証する手段と、操作権が登録のものと一致するかを確認する手段とを有し、正当な権利をもち、かつ、操作権をもっているユーザからのデータのみを、制御系用リアルタイムオペレーティングシステム上で動作するプロセスにプロセス間通信し、制御系用リアルタイムオペレーティングシステム上では、さらに、制御コマンドを実行することが許可されている操作権であるかを確認する手段を有していることを特徴とする制御系用ファイアウォール。

【請求項５】請求項１記載の制御系用ファイアウォールであって、制御系用リアルタイムオペレーティングシステム上では、制御コマンドを前記監視制御用コンピュータに通信したとき、該監視制御用コンピュータより制御コマンドに対する進捗状況、または、結果を受信し、該進捗状況、または、結果を情報系用オペレーティングシステム上で動作するプロセスにプロセス間通信する手段を有し、情報系用オペレーティングシステム上では、プロセス間通信によって入手した進捗状況、または、結果を制御コマンドの発信元に転送する手段とを有していることを特徴とする制御系用ファイアウォール。

2

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、不特定多数の人が利用する情報系ネットワークを利用して、プラントの監視制御を行うシステムにおいて、情報系ネットワークと制御系ネットワークとを安全に接続する装置に関する。

【０００２】

【従来の技術】従来、例えば、下水処理場や排水機場などのプラントの監視制御は、専用のリアルタイムオペレーティングシステム（以下、ＲＴ－ＯＳという）で動作する制御機器・計測機器・制御装置・監視制御卓などを専用の回線で接続して制御系ネットワークを構築し、専用の制御系用通信プロトコルによって制御データ・監視データなどを通信する送ることによって行われてきた。

【０００３】これに対し、企業をはじめとする様々な組織では、事務管理や電子メール・プリンタの共有などを目的として、組織内情報系ネットワーク（以下、イントラネットという）を構築している。一般に、情報端末には汎用のオペレーティングシステム（以下、Ｇ－ＯＳという）で動作するものを利用し、また、汎用の情報通信用プロトコルによって情報通信を行っている。さらに、イントラネットをインターネットに接続して、組織を超えたＷＷＷ（Ｗｏｒｌｄ　Ｗｉｄｅ　Ｗｅｂ）サービスや電子メールも行っている。

【０００４】インターネットを経由して、イントラネットに不正な侵入を防ぐものとしてファイアウォールがある。例えば、文献１（「ファイアウォール」、５１頁～７９頁、１９９５、ソフトバンク）によれば、ファイアウォールには、方式として、パケットフィルタリングゲートウェイ、トランスポートレベルゲートウェイ、アプリケーションレベルゲートウェイがある。

【０００５】パケットフィルタリングゲートウェイは、送信元／送信先のＩＰ（Ｉｎｔｅｒｎｅｔ　Ｐｒｏｔｏｃｏｌ）アドレス／ポートに基づいてパケットを遮断／許可する。トランスポートレベルゲートウェイは、送信元がトランスポートレベルゲートウェイのＴＣＰ（Ｔｒａｎｓｍｉｓｓｉｏｎ　Ｃｏｎｔｒｏｌ　Ｐｒｏｔｏｃｏｌ）ポートに接続すると、トランスポートレベルゲートウェイが別のネットワーク上のサーバのポートに接続する。コネクションが確立している間は、トランスポートレベルゲートウェイがリレーして、すべてのデータが

双方向に送られる。アプリケーションレベルゲートウェイは、送信元が別のネットワーク上のサーバのポートに接続要求をしたとき、アプリケーションレベルゲートウェイのＴＣＰポートに接続し、アプリケーションレベルゲートウェイが要求のあったサーバのポートに接続要求する。

【０００６】こうした状況において、制御系ネットワークとイントラネットとを接続し、情報系ネットワーク上の情報端末（イントラネット内の情報端末、インターネットを介して接続する情報端末、公衆回線・無線などを使ってイントラネットに接続した情報端末など）からプラントの監視・制御、または、プラントの監視データの２次利用を行うシステムが要求されている。

【０００７】上記のシステムを構築するためには、（１）従来の制御系ネットワーク、および、制御用通信プロトコルを、情報系ネットワーク、および、情報系通信プロトコルに置き換えて再構築する方法と、（２）従来の制御系ネットワーク、および、制御用通信プロトコルを使って独自のイントラネットを構築し、その上に情報端末を接続する方法と、（３）従来の制御系ネットワーク、とイントラネットとを接続する方法とがある。このうち、（１）（２）は既に稼動しているプラント監視制御系、または、イントラネットを再構築する必要が生じ、それぞれに必要なサービスを業務に支障をきたさないように維持するのは大変である。また、いずれかが新規の構築になる場合であっても、それぞれに必要なサービスが一様に同一のネットワーク上にあることは、制御系の役割を考えると、セキュリティやリアルタイム性の点で不安である。そこで、図２に示すように、制御系ネットワーク１０００と情報系ネットワーク２０００とを分けて考え、それらを接続する。このとき、制御系のセキュリティやリアルタイム性を確保するために、制御系ネットワーク１０００と情報系ネットワーク２０００との接点に、制御系用ファイアウォール１が必要となる。

【０００８】制御系用ファイアウォール１には、制御系ネットワークに接続するための制御系ＬＡＮボード、および、情報系ネットワークに接続するための情報系ＬＡＮボードを搭載し、制御系用通信プロトコルと、情報系用通信プロトコルとがサポートされている必要がある。両通信プロトコルをサポートするためには、ＲＴ－ＯＳに両通信プロトコルをサポートさせる方法と、Ｇ－ＯＳとＲＴ－ＯＳの両方を共存させる方法が考えられる。

【０００９】Ｇ－ＯＳとＲＴ－ＯＳの両方を共存させる方法としては、例えば、文献２（「リアルタイム制御方式」、特開平１０－２１０９４）によれば、Ｇ－ＯＳが動作するＣＰＵと、ＲＴ－ＯＳが動作するＣＰＵとを搭載し、共有メモリを介して相互のプロセスの間のデータ交換を行う方法と、ＲＴ－ＯＳをコアにして、この上にＧ－ＯＳエミュレータを実装する方法とが紹介されている。

【００１０】

【発明が解決しようとする課題】本発明の課題は、プラントの監視制御を行う制御系ネットワークと組織内情報系ネットワーク（イントラネット）を接続し、イントラネット上の情報端末などで、プラントデータの監視、または、プラントの制御を行うとき、制御系ネットワークのセキュリティ、および、リアルタイム性を確保するために、制御系ネットワークとイントラネットの接点に設置する制御系用ファイウォールを提供することにある。

【００１１】本発明の第１の課題は、制御系にとって有用なコマンドのみを制御系に転送するコマンドフィルタリング機能を有する制御系用ファイアウォールを提供することにある。

【００１２】本発明の第２の課題は、制御系の状況に応じて有用なコマンドの制限を変更するアクティブコマンドフィルタリング機能を有する制御系用ファイアウォールを提供することにある。

【００１３】本発明の第３の課題は、コマンドフィルタリングのルールを情報系ネットワーク上のいかなるプロセスからも覗くことができないようにするフィルタリングテーブル不可視化機能を有する制御系用ファイアウォールを提供することにある。

【００１４】本発明の第４の課題は、権利のないユーザが制御できないように、かつ、権利をもつユーザでも他の権利者が制御を実行している間は制御できないようにするユーザ認証・操作権認証機能を有する制御系用ファイアウォールを提供することにある。

【００１５】本発明の第５の課題は、制御コマンドを送信したとき、そのコマンドに対する制御系の進捗状況、または、結果をレポートするトランザクションモニタリング機能を有する制御系用ファイアウォールを提供することにある。

【００１６】本発明の第６の課題は、不特定多数のユーザがプラントデータの監視ができ、かつ、不特定多数のリクエストが制御系にじょう乱を与えないようにするリアルタイム監視データ転送機能を有する制御系用ファイアウォールを提供することにある。

【００１７】本発明の第７の課題は、プラント監視データのヒストリカルデータも不特定多数のユーザが利用できるようにするリアルタイム監視データ転送機能を有する制御系用ファイアウォールを提供することにある。

【００１８】本発明の第８の課題は、プラント監視データをリアルタイムに必要とするユーザに対して、ユーザが毎回リクエストを要求しなくてもデータが配信され、かつ、要求のないプラント監視データはデータが配信されないようにするリアルタイム監視データ転送機能を有する制御系用ファイアウォールを提供することにある。

【００１９】本発明の第９の課題は、故障などのイベントが発生したときに、不特定多数のユーザに対してリアルタイムに配信され、かつ、後でイベント発生リストを

確認することもできるようにするリアルタイム監視データ転送機能を有する制御系用ファイアウォールを提供することにある。

【００２０】本発明の第１０の課題は、ＲＴ－ＯＳとＧ－ＯＳとの双方に対して、メモリや記憶装置、ＬＡＮボードなどに対して、アクセス領域が異なる制御系用ファイアウォールを提供することにある。

【００２１】本発明の第１１の課題は、制御系用ファイアウォール上に対するアクセスによって発生した事象を、不正・正当を問わずログをとる機能と、そのログを分析して適当な警報システムに状況報告をする機能を有する制御系用ファイアウォールを提供することにある。

【００２２】

【課題を解決するための手段】（１）制御系用ファイアウォールをＧ－ＯＳとＲＴ－ＯＳが共存するコンピュータに実装する。Ｇ－ＯＳとＲＴ－ＯＳ上のそれぞれのプロセスは共有メモリを介してプロセス間通信ができるようにする。このとき、Ｇ－ＯＳ上の情報系プロセスで、暗号化データを受信し、そのデータを復号化し、復号化したデータをＲＴ－ＯＳ上の制御系プロセスに渡す。この制御系プロセスで、データから制御コマンドを抽出し、コマンドフィルタリングテーブルを参照して、「通過」できるコマンドだけを制御系ＬＡＮ上の監視制御コンピュータなどに転送する。

【００２３】（２）監視制御コンピュータなどからの監視データに基づいて、コマンドフィルタリングテーブルのルールを変更するロジックをもつプロセスをＲＴ－ＯＳ上で実行させるか、または、監視制御コンピュータなどから直接ルールの変更要求を受け取れるようにする。

【００２４】（３）コマンドフィルタリングテーブルをＧ－ＯＳ上の情報系プロセスからはアクセスできないメモリや記憶装置におく。

【００２５】（４）情報系プロセスにおいて、正当なユーザからのアクセスであるかを認証し、正当なユーザからのアクセスの場合、正当なユーザが利用している端末と制御系用ファイウォール１との間でユニークな操作権番号を共有する。正当なユーザからの暗号化データを受信するが、それには、「ユーザＩＤ」「操作権番号」「制御コマンド」が含まれるようにする。そして、ユーザＩＤと操作権番号が一致するかをチェックする。もし、一致するならば、「操作権番号」と「制御コマンド」を制御系プロセスに転送する。制御系プロセスでは、「操作権番号」と「制御コマンド」を含むデータを受信し、操作権認証を行う。操作権認証は、受信した「操作権番号」と「制御コマンド」の組み合わせが一致するかを比較する。

【００２６】（５）制御系プロセスで、正当な制御コマンドを監視制御コンピュータなどに転送した後、制御コマンドを送出したことをプロセス間通信によって、情報系プロセスに通知し、情報系プロセスは、通知を受け取ると、さらに、制御コマンドを発信したユーザ宛てに転送する。このサイクルを監視制御コンピュータなどから制御トランザクションに関するレポートが通知されるたびに繰り返す。

【００２７】（６）制御系プロセスで監視データを受信したとき、プロセス間通信で情報系プロセスに監視データを引き渡し、さらに、情報系プロセスは、情報系ＬＡＮ上の端末やデータベースサーバに監視データを転送する。

【００２８】（７）情報系プロセスにおいて、タイマーを設定し、前回、データを転送したときの転送時刻よりも新しい時刻のものに更新されているものだけを取り出し、データベースサーバへまとめて転送する。そして転送時刻を更新する。

【００２９】（８）情報系プロセスにおいて、ユーザから、ある監視項目のリアルタイム配信要求を受けたとき、正当なユーザからの要求であるかを認証を行う。正当なユーザである場合には、その監視項目と配信先を登録する。この登録が済むと、指定されている監視項目の更新がある度に、登録されている配信先へ監視データを転送する。

【００３０】（９）情報系プロセスにおいて、イベント発生を受信する度に、イベント内容を情報系ＬＡＮ上にマルチキャストする。

【００３１】（１０）共有メモリに、Ｇ－ＯＳから書き込み可能だが、ＲＴ－ＯＳからは読み込みしかできないアドレス空間と、ＲＴ－ＯＳから書き込み可能だが、Ｇ－ＯＳからは読み込みしかできないアドレス空間とを持たせる。

【００３２】また、Ｇ－ＯＳからしかアクセスできないメモリや記憶装置、ＬＡＮボード、及び、ＲＴ－ＯＳからしかアクセスできないメモリや記憶装置、ＬＡＮボードを持たせる。

【００３３】（１１）情報系プロセスにおいて、受信したデータを復号化したとき、送信元、ユーザ名、アクセス時刻、内容、処理状況のログをとる。定期、または、不定期に、このアクセスログを分析すし、分析によってアクセス状況を認識し、重大、または、注意に値する状況になっている場合には、警報システムへ状況を報告する。

【００３４】

【発明の実施の形態】図２は、制御系用ファイアウォールを介して情報系ネットワークと制御系ネットワークを接続するシステム構成例を示したものである。

【００３５】制御系用ファイアウォール（プラントファイアウォール）１は、制御系ネットワーク（制御系ＬＡＮ）１０００と、情報系ネットワーク（イントラネット）２０００との間に接続される。制御系ＬＡＮ１０００には、監視制御コンピュータ１００１が接続され、監視制御コンピュータ１００１は、制御機器１００２の制

御を行ったり、計測機器１００３の計測データを取り込んだりしている。監視制御卓１００４は制御コマンドの送信やデータの監視を行う。イントラネット２０００には、情報サーバ２００３、データベースサーバ２００４、情報端末３００１などが接続され、さらに、ファイアウォール２００２を介してインターネット２００１に接続している。情報端末３００１としては、イントラネット２０００上の他にも、公衆回線や無線回線など３００２を介して情報サーバ２００３の１つに接続するもの、インターネットサービスプロバイダ３００３を介してインターネットに接続しているもの、他のネット上からインタネットに接続しているものなどがある。

【００３６】図１、３、４、５は、制御系用ファイアウォールの第１の発明であるコマンドフィルタリング機能の実施例を示したものである。

【００３７】制御系用ファイアウォール１は、制御系ＬＡＮに接続する制御系ＬＡＮボード１４と、イントラネットに接続する情報系ＬＡＮボード１１とを搭載し、ＲＴ－ＯＳ３とＧ－ＯＳ２とが動作し、それぞれのＯＳ上で、制御系用通信プロトコルによる通信９、情報系用通信プロトコルによる通信４で通信する機能を持っている。さらに、ＲＴ－ＯＳ上のプロセス３０とＧ－ＯＳ上のプロセス２０は、制御系－情報系間プロセス通信機能６、７によって共有メモリ１０を介してプロセス間通信することができる。なお、図３以降の発明に関する図においては、通信プロトコル４、９、プロセス間通信６、７、メモリ・記憶装置など管理５、８に該当するものは割愛する。

【００３８】情報系プロセス２０では、暗号化データを受信し（２１）、復号鍵を使って暗号化データを復号化する（２２）。正当なデータならば、復号化データには制御コマンドが含まれている。そして、復号化データの一部、または、全部（制御コマンドを含む）を制御系－情報系間プロセス通信を使って制御系プロセス３０に渡す（２３）。制御系プロセス３０で復号化データの一部、または、全部を受信し（３１）、復号化データの中から制御コマンドをとりだし、その制御コマンドの通過・待機・遮断を行うコマンドフィルタリングを行い（３２）、通過させる制御コマンド（正当なコマンド）のみを制御系ＬＡＮ上の監視制御用コンピュータ１００１などに転送する。

【００３９】図３は、コマンドフィルタリングを行うためのフイルタリングテーブル３４の例を示したものである。

【００４０】フィルタリングテーブル３４には、フィルタリング動作４１、制御コマンド４２、制御コマンドの送信先４３が記述されており、ＲＴ－ＯＳ３上のプロセス上から読み書き可能なメモリ、または、ハードディスクなどの記憶装置１３に記憶されている。動作には、「通過」「待機」「遮断」がある。

【００４１】図４、５は、コマンドフィルタリング３２の具体的処理を示したものである。

【００４２】受信した復号化データから抽出した制御コマンドがフィルタリングテーブル３４に存在しているかを確認し（５１）、コマンドが存在していない場合は、削除して（５４）、終了する。存在する場合は、フィルタリング動作をチェックする（５２）。動作が「遮断」のコマンドは、削除して（５４）、終了する。「通過」のコマンドは、監視制御コンピュータなど指定されている送信先に送信する（３３）。「待機」のコマンドは、コマンドの内容を保持し、別プロセスなどからの通知を待つ（５３）。もし、別プロセスから通知があり、動作が「待機」から「通過」または「遮断」に変更になったときは、フィルタリング動作の再チェックを行う（５２）。

【００４３】しかし、もし、あるコマンドが連続して送信されたとき（制御トランザクションが完了しないうちに次のコマンドが送信されたとき）に、図４の処理だけでは不足である。そこで、図５に示したように、「通過」のコマンドに対しては、まず、そのフィルタリングルールの動作を一時「待機」にしておき（５５）、コマンドを転送した（３３）後、制御トランザクションの完了を待って（５６）、完了を知った時点で、また、「通過」に戻す（５７）。連続して送信されたコマンドは「待機」に基づき保持される。

【００４４】以上によって、情報系ＬＡＮ上の情報端末から行える制御を限定できる。不必要な制御コマンドがいたずらに制御系ＬＡＮ上に流れることもない。制御トランザクションが完了しないうちに到着した制御コマンドにも対処できる。もし、一切の制御コマンドを排除したい場合には、フィルタリングテーブルの中味を無にすれば良い（記述のない制御コマンドは「遮断」を意味する）。

【００４５】図６は、制御系用ファイアウォールの第２の発明であるアクティブコマンドフィルタリング機能の実施例を示したものである。

【００４６】制御系プロセス６０で、監視データ、または、フィルタリング動作変更要求を取得する（６１）。フィルタリング動作変更要求（コマンドＡを「通過」など）を取得した場合には、その通りにフィルタリングテーブルの変更を行う（６３）。制御系プロセス６０からアクセス可能なメモリまたは記憶装置１３上に、フィルタリング動作を変更するためのルール６５が存在する場合には、これに従って、入手した監視データを元に、動作変更の必要性があるかを調べ（６２）、必要がある場合には、フィルタリングテーブルの変更を行う（６３）。変更を行ったときは、別の制御系プロセスにもその旨を通知する（６４）。フィルタリング動作を変更するためのルール６５とは、例えば、「主電源がＯＦＦ状態のとき、緊急ポンプ停止の制御コマンドは遮断」など

のルールである。

【００４７】監視制御コンピュータ１００１側が、有効な制御コマンドを管理する機能を既にもっている場合（つまり、制御プロセス６０の中の、動作変更要求の必要性の判断を行うロジック６２相当のものを既に監視制御コンピュータが持っている場合）は、制御コマンドの有効／無効が切り替わったときのみ、その旨を制御系用ファイアウォール１に送信し、そのコマンドに対する動作の通過／遮断を切り替えることができる。監視制御コンピュータ１００１側が、有効な制御コマンドを管理する機能を持っていない場合には、２つの方法がある。

（１）監視制御コンピュータにロジックを実装する。

（２）制御系用ファイアウォール１の制御系プロセス６０に実装する。（２）の場合、例えば、制御系ＬＡＮ上にたくさんの監視制御コンピュータがある場合でも、ロジックのメンテナンスを１箇所で行うことができる。逆に、ロジックが複雑、または、ルールを処理する数が多いと、制御系用ファイアウォール自身の負荷が大きくなる。

【００４８】以上によって、例えば、ポンプ運転の状態に入ったら、保守コマンド系は遮断するとか、電源がＯＮの状態でないと、ポンプ運転系のコマンドは受け付けないなど、制御系の状態に基づく制御コマンドのフィルタリングができる。つまり、制御系の現在状態にとって不必要な制御コマンドがいたずらに制御系ＬＡＮ上に流れることを防げる。

【００４９】図７は、制御系用ファイアウォールの第３の発明であるフィルタリングテーブルの不可視化の実施例を示したものである。

【００５０】Ｇ－ＯＳ２とＲＴ－ＯＳ３が動作する制御系用ファイアウォールに対して、フィルタリングテーブルの記憶は、（ａ）情報系プロセスからアクセス可能なメモリ、記憶装置１２上、（ｂ）情報系プロセスからアクセス可能な共有メモリ１０上、（ｃ）制御系プロセスからアクセス可能なメモリ、記憶装置１３上の３つがある。

【００５１】（ａ）の場合、情報系プロセス７０ａからアクセス可能なため、悪意のあるユーザによって例えばシステムのルート権限に不正侵入して、フィルタリングテーブル７２ａを書き換えてしまう可能性がある。フィルタリングテーブルが読み込みしかできないようになっている場合は、動的にフィルタリングテーブルを変更することができなくなる。また、読み込みができることを利用して、制御可能なコマンドをいたずらに送信してくる可能性もでてしまう。

【００５２】（ｂ）の場合も（ａ）と同様の問題がある。

【００５３】これに対し、（ｃ）の場合、情報系プロセス７０ｃからは、直接的には、フィルタングテーブルを参照することができないので、情報系ＬＡＮ上の端末からは、制御可能なコマンド書き換えられることも、盗み見られることも可能性は極めて小さい。

【００５４】第３の発明は、フィルタリングテーブル７３を制御系プロセス７１からのみアクセス可能なメモリ、記憶装置１３上に記憶することで情報系プロセスから隠ぺいすることができる。

【００５５】図８、９、１０、１１は、制御系用ファイアウォールの第４の発明であるユーザ認証・操作権認証機能の実施例を示したものである。

【００５６】情報系プロセス８０は、ユーザＩＤとパスワードとの組み合わせなどを用い、正当なユーザからのアクセスであるかを認証する（８１）。そして、正当なユーザからのアクセスと判断されたときは、正当なユーザが利用している端末３００１と制御系用ファイウォール１との間でユニークな操作権番号８４、８５を共有する（８２）。このとき、制御系用ファイアウォール１側ではユーザＩＤと操作権番号の組み合わせを暗号化して記憶しておくことが望ましい（８３）。もし、同じユーザＩＤを使って別の端末からもアクセスがあるとしても、別の操作権番号が共有されることになる。

【００５７】次に、情報系プロセス９０は、正当なユーザからの暗号化データを受信し（２１）、復号化する（２２）。復号化したデータには、「ユーザＩＤ」「操作権番号」「制御コマンド」が含まれる。そして、ユーザＩＤと操作権番号が一致するかをチェックする（９１）。もし、一致するならば、「操作権番号」と「制御コマンド」を制御系プロセスに転送する（２３）。

【００５８】制御系プロセス１００は、「操作権番号」と「制御コマンド」を含む復号化データを受信し（３１）、操作権認証を行ってから（１０１）、コマンドフィルタリングを行う（３２）。このとき、図１１に示したようにフィルタリングテーブル３４には、制御コマンド４２に対する操作権番号１０４が記憶されている。図中「－」で示されているのは、その制御コマンドが現在どのユーザにも利用しようとしていないことを意味する。操作権認証１０１は、受信した「操作権番号」と「制御コマンド」の組み合わせが一致するかを比較する（１０２）。もし、一致するならば、コマンドフィルタリングを行う（３２）。もし、フィルタリングテーブルに操作権番号が登録されていないとき（図中「－」のとき）は、受信した操作権番号を該当の制御コマンド、および、それに関連する制御コマンドに登録をしてから（１０３）、コマンドフィルタリングを行う（３２）。一致しないときは終了する。

【００５９】その他に、制御系プロセスには、制御系コマンドと操作権番号との関連付けを空きにする手順が必要である。これは、利用者が操作権を放棄したり、または、一定時間以上操作がない（操作権の放棄の忘れ）、または、ある利用者の操作権を強制的にはく奪する場合に実行される。

【００６０】以上によって、制御系にコマンドを送り込むことができるのは、正当なユーザだけである。しかも、他の正当なユーザが制御コマンドを実施中は、例え、自分が正当ユーザであっても、制御コマンドを送り込むことはできない。図１２は、制御系用ファイアウォールの第５の発明であるトランザクションモニタリング機能の実施例を示したものである。

【００６１】制御系プロセス１１０では、正当な制御コマンドを転送した後（３３）、制御コマンドを送出したことをプロセス間通信によって、情報系プロセス１２０に通知する（１１１）。情報系プロセスでは、通知を受け取ると、その内容を、さらに、制御コマンドを発信したユーザ宛てに転送する（１２２）。このサイクルを監視制御コンピュータなどから制御トランザクションに関するレポートが通知されるたびに繰り返し（１１３、１２１）、制御トランザクションが完了するまで繰り返す（１１２、１２３）。

【００６２】以上によって、ユーザが送信した制御コマンドが正確に監視制御コンピュータ１００１などに伝わったのかを把握することができる。また、１つの制御コマンドに対してその制御トランザクションが完了するのに時間がかかる場合でも途中の進捗状況を把握することができる。

【００６３】図１３、１４は、制御系用ファイアウォールの第６の発明である監視データ転送機能の実施例を示したものである。

【００６４】制御系プロセス１３０では、監視データを制御系ＬＡＮ上の監視制御コンピュータなどから受信し（１３１）、監視データをプロセス間通信によって、情報系プロセスに渡す（１３２）。実際には、図１４に示したように共有メモリ１０上の監視データ空間１３４に書き込まれ、ここには最新データ、及び、その更新時刻などの可変データが入る。一方、共有メモリ１０上には、監視項目に対する属性情報空間１３３もあり、ここには、データＩＤ、データ名称、単位、共有メモリ上の監視データの保存アドレスなどが示される。属性情報空間１３３の内容は、監視項目の追加や削除・修正などがあった場合に制御系プロセス側から書き換えられるようになっている。

【００６５】情報系プロセス１４０では、監視データを受信した後（１４１）、監視データを情報系ＬＡＮ上の端末３００１やデータベースサーバ２００４などにさらに転送する（１４２）。また、必要に応じて、属性情報空間の内容を転送する場合もある。

【００６６】以上によって、監視制御コンピュータ１００１などがもつ制御機器や計測機器のデータを情報系上の端末やデータベースサーバに転送することができる。

【００６７】上記の監視データの情報系ＬＡＮ上の機器への転送の方法には、さらに、以下の３つの発明がある。

【００６８】図１５、１６は、監視データの転送機能における大容量データ転送機能の発明（制御系用ファイアウォールの第７の発明）の実施例を示したものである。

【００６９】まず、タイマーイベントを発生する初期時刻、及び、時間間隔１５９をセットしておく（１５１）。

【００７０】情報系プロセス１５０では、タイマーイベントが発生すると（１５２）、前回、データをデータベースサーバ２００４へ転送したときの転送時刻１５８を読み込む（１５３）。監視データを受信し（共有メモリ１０上のデータを読み込み）（１４１）、前回転送時刻よりも新しい時刻のデータであるかをチェックする（１５４）。データが新しいときは、そのデータを一時記憶する（１５５）。これをすべての監視データに対して繰り返す（１５６）。そして、一時記憶しておいた監視データをデータベースサーバ２００４へまとめて転送する（１４２）。転送した監視データの中で最も新しい更新時刻を最終転送時刻１５８として書き換える（１５７）。

【００７１】上記を図１６の具体的な例で説明する。この例では、１２：００を基点として、２０分ごとにタイマーイベントが発生するように設定されてあり、現在時刻は、１３：２０になった場合である。前回の最終転送時刻は１３：００と記憶されており、監視データ空間１３４上のデータから１３：００よりも新しいものを一時記憶空間１６４に抽出し、抽出したデータをまとめてデータベースサーバに転送する。そして、最終転送時刻を最も新しいものである１３：１５におきかえる。なお、この例において、最終転送時刻を現在時刻の１３：２０とする場合もある。

【００７２】以上によって、データベースサーバ２００４に定期的にデータを一括して転送することができる。監視データ空間のデータの更新時刻が同一でなくても問題ない。このとき、更新されていないデータに関しては、転送されないので、トラフィックの節約にもなるし、一度送ったことのあるデータの再送によるデータベースサーバ側の負荷低減にもなる。また、通常、制御系上での監視データの更新サイクルはかなり短く、このサイクルに合わせて全てのデータを転送するのは、相当負荷が大きいが、時間間隔の設定ができるので、転送サイクルを長くすることで、制御系プラントファイウォール・ネットワークトラフィック・データベースサーバの負荷を抑えることができる。

【００７３】図１７は、監視データの転送機能におけるリアルタイム配信機能の発明（制御系用ファイアウォールの第８の発明）の実施例を示したものである。

【００７４】情報系プロセス１６０では、ある監視項目のリアルタイム配信要求を受信すると（１６１）、まず、そのユーザの認証を行う（８１）。正当なユーザである場合には、その監視項目と配信先を登録する（１６

２）。

【００７５】上記の登録があると、情報系プロセス１４０では、指定されている監視項目の更新がある度に（１４１）、登録されている配信先へ転送する（１４２）。なお、配信先は１箇所でない場合もある。

【００７６】以上によって、情報系ＬＡＮ上の端末は、リアルタイム配信を受けることができる。また、ユーザ認証を加えていることにより、なりすましによってリアルタイム配信サービスを不正に大量に行って、リアルタイム配信サービスの妨害することから防ぐこともできる。なお、リアルタイム配信は、１ユーザあたり３項目までのように制約をつけてリアルタイム配信サービスを保護してもよい。

【００７７】図１８は、監視データの転送機能におけるイベントのマルチキャスト配信機能の発明（制御系用ファイアウォールの第９の発明）の実施例を示したものである。

【００７８】情報系プロセス１７０では、イベント発生を受信する度に（１７１）、イベント内容を情報系ＬＡＮ上にマルチキャストする（１７２）。情報系ＬＡＮ上のデータベースサーバ２００４、端末３００１はマルチキャストを受信すると、イベント内容を取り込み、データベースサーバにイベントを取り込んだり、端末にイベントを表示したりなどの適切な処置を行う。

【００７９】以上によって、マルチキャストを受信する体制になっている情報系ＬＡＮ上の端末、データベースサーバは、イベントをリアルタイムに受信することができる。また、端末が受信する体制になかったとしても、データベースサーバには、発生イベントが格納されているので、こちらを参照することでイベントリストを見ることができる。

【００８０】図１９は、制御系用ファイアウォールの第１０の発明であるメモリアクセスの安全性の実施例を示したものである。

【００８１】制御系用ファイアウォール１は、Ｇ－ＯＳ２とＲＴ－ＯＳ３が実装され、それぞれ共有メモリ１０にアクセスすることができる。このとき、共有メモリは、Ｇ－ＯＳ２から書き込み可能だが、ＲＴ－ＯＳ３からは読み込みしかできないアドレス空間１８１と、ＲＴ－ＯＳ３から書き込み可能だが、Ｇ－ＯＳ２からは読み込みしかできないアドレス空間１８２とを持たせる。アドレス空間１８１には、例えば、制御コマンドや、適当な各種フラグが、Ｇ－ＯＳ側のプロセスによって書き込まれる。アドレス空間１８２には、例えば、属性情報や、適当な各種フラグ、監視データ、イベント、制御トランザクションのレポートなどが、ＲＴ－ＯＳ側のプロセスによって書き込まれる。

【００８２】以上によって、Ｇ－ＯＳ上のプロセスが誤って、監視データやイベントなどを書き換えてしまうことがなくなる。また、共有メモリを介したプロセス間通信として、お互いに通信の受領を通知したい場合でも、両方の空間にそれぞれのＯＳのプロセスがフラグを書き込むための領域があるので、問題ない。

【００８３】図２０は、制御系用ファイアウォールの第１１の発明であるメモリアクセスの安全性の第2の実施例を示したものである。

【００８４】制御系用ファイアウォール１は、Ｇ－ＯＳ２とＲＴ－ＯＳ３が実装され、それぞれ共有メモリ１０にアクセスすることができるが、Ｇ－ＯＳ２からしかアクセスできないメモリや記憶装置１２、ＬＡＮボード１１、及び、ＲＴ－ＯＳ３からしかアクセスできないメモリや記憶装置１３、ＬＡＮボード１４を持たせる。例えば、Ｇ－ＯＳ２は、メモリ１３を認識することはできない。

【００８５】以上によって、例えば、コマンドフィルタリングテーブル３４をメモリ１３に置くことで、Ｇ－ＯＳ側のプロセスからは、その内容を直接読んだり、書き換えたりすることはできない。

【００８６】図２１は、制御系用ファイアウォールの第１２の発明であるアクセスログ機能の実施例を示したものである。

【００８７】情報系プロセス１９０では、暗号化してある、または、平文のままのデータを受信する（２１）。そして、その内容を復号化する（２２）。当然、平文は復号化処理を施せば意味のないものにかわる。そして、復号化したデータが、意味のあるものかどうかを判断し（１９１）、意味不明の場合には、内容が不正であるとして、処理を「不正による削除（１９２）」として、送信元、ユーザ名、アクセス時刻、内容、処理状況のログ１９５をとる（１９４）。復号化した内容に意味がある場合には、ユーザＩＤや操作権番号が一致するかを確認し（９１）、不一致の場合には、「処理：操作権不一致による削除（１９３）」として、同様にログ１９５をとる（１９４）。一致の場合には、「処理：正当なデータ転送」として、内容をプロセス間通信によって、制御系プロセスに引き渡す。このときもログ１９５をとる（１９４）。

【００８８】図２２は、制御系用ファイアウォールの第１３の発明である警報機能の実施例を示したものである。

【００８９】情報系プロセス２００では、定期、または、不定期に、アクセスログ１９５を分析する（２０１）。分析によってアクセス状況を認識し（２０２）、もし、重大、または、注意に値する状況になっている場合には、警報システムへ状況を報告する（２０３）。問題なければ、特に何もしない。

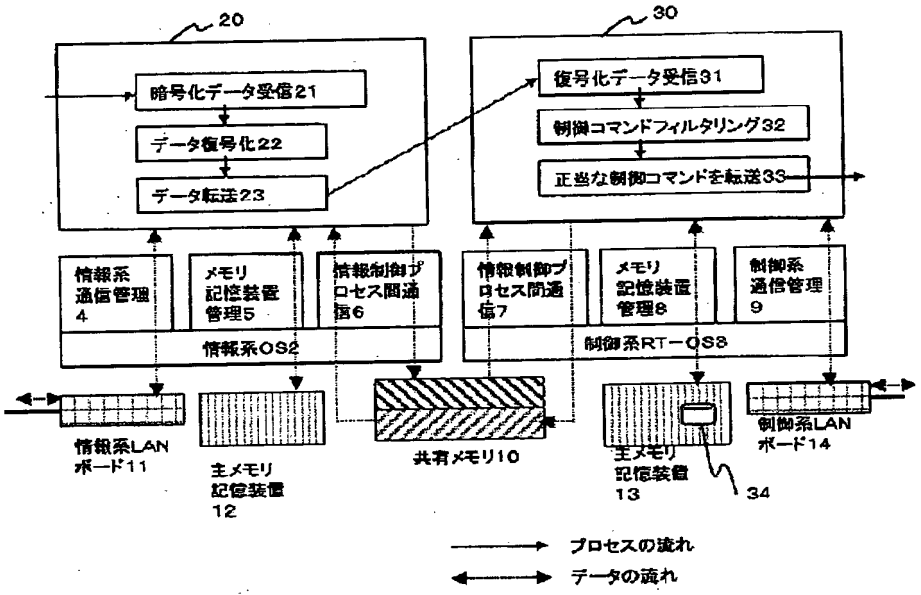
【００９０】以上によって、正当、不正を含めてアクセスの状況が内容レベルまでログをとり、さらに、重大な不正があった場合には、即座に警報システムに報告がでる。

【００９１】
【発明の効果】本発明によれば、情報系ＬＡＮ上の情報端末３００１から行える制御を限定できる。不必要な制御コマンドがいたずらに制御系ＬＡＮ上に流れることもない。制御トランザクションが完了しないうちに到着した制御コマンドにも対処できる。もし、一切の制御コマンドを排除したい場合には、フィルタリングテーブルの中味を無にすれば良い。
【００９２】本発明によれば、例えば、ポンプ運転の状態に入ったら、保守コマンド系は遮断するとか、電源がＯＮの状態でないと、ポンプ運転系のコマンドは受け付けないなど、制御系の状態に基づく制御コマンドのフィルタリングができる。つまり、制御系の現在状態にとって不必要な制御コマンドがいたずらに制御系ＬＡＮ上に流れることを防げる。
【００９３】本発明によれば、フィルタリングテーブルを制御系プロセスからのみアクセス可能なメモリ、記憶装置上に記憶することで情報系プロセスから隠ぺいすることができる。
【００９４】本発明によれば、制御系にコマンドを送り込むことができるのは、正当なユーザだけである。しかも、他の正当なユーザが制御コマンドを実施中は、例え、自分が正当ユーザであっても、制御コマンドを送り込むことはできない。本発明によれば、ユーザが送信した制御コマンドが正確に監視制御コンピュータなどに伝わったのかを把握することができる。また、１つの制御コマンドに対してその制御トランザクションが完了するのに時間がかかる場合でも途中の進捗状況を把握することができる。
【００９５】本発明によれば、監視制御コンピュータなどがもつ制御機器や計測機器のデータを情報系上の端末やデータベースサーバに転送することができる。
【００９６】本発明によれば、データベースサーバに定期的にデータを一括して転送することができる。監視データ空間のデータの更新時刻が同一でなくても問題ない。このとき、更新されていないデータに関しては、転送されないので、トラフィックの節約にもなるし、一度送ったことのあるデータの再送によるデータベースサーバ側の負荷低減にもなる。また、通常、制御系上での監視データの更新サイクルはかなり短く、このサイクルに合わせて全てのデータを転送するのは、相当負荷が大きいが、時間間隔の設定ができるので、転送サイクルを長くすることで、制御系プラントファイウォール・ネットワークトラフィック・データベースサーバの負荷を抑えることができる。
【００９７】本発明によれば、情報系ＬＡＮ上の端末は、リアルタイム配信を受けることができる。また、ユーザ認証を加えていることにより、なりすましによってリアルタイム配信サービスを不正に大量に行って、リアルタイム配信サービスの妨害することから防ぐこともできる。
【００９８】本発明によれば、マルチキャストを受信する体制になっている情報系ＬＡＮ上の端末、データベースサーバは、イベントをリアルタイムに受信することができる。また、端末が受信する体制になかったとしても、データベースサーバには、発生イベントが格納されているので、こちらを参照することでイベントリストを見ることができる。
【００９９】本発明によれば、Ｇ－ＯＳ上のプロセスが誤って、監視データやイベントなどを書き換えてしまうことがなくなる。また、共有メモリを介したプロセス間通信として、お互いに通信の受領を通知したい場合でも、両方の空間にそれぞれのＯＳのプロセスがフラグを書き込むための領域があるので、問題ない。
【０１００】本発明によれば、例えば、コマンドフィルタリングテーブルをメモリに置くことで、Ｇ－ＯＳ側のプロセスからは、その内容を直接読んだり、書き換えたりすることはできない。
【０１０１】本発明によれば、正当、不正を含めてアクセスの状況が内容レベルまでログをとり、さらに、重大な不正があった場合には、即座に警報システムに報告がでる。
【図面の簡単な説明】
【図１】本発明のコマンドフィルタリング機能の実施例の説明図である。
【図２】制御系用ファイアウォールを含めた全体システムの例である。
【図３】本発明のコマンドフィルタリング機能の実施例の第１の説明図である。
【図４】本発明のコマンドフィルタリング機能の実施例の第２の説明図である。
【図５】本発明のコマンドフィルタリング機能の実施例の第３の説明図である。
【図６】本発明のアクティブコマンドフィルタリング機能の実施例の説明図である。
【図７】本発明のコマンドフィルタリングテーブルの不可視化の実施例の説明図である。
【図８】本発明のユーザ認証・操作権認証機能の実施例の第１の説明図である。
【図９】本発明のユーザ認証・操作権認証機能の実施例の第２の説明図である。
【図１０】本発明のユーザ認証・操作権認証機能の実施例の第３の説明図である。
【図１１】本発明のユーザ認証・操作権認証機能の実施例の第４の説明図である。
【図１２】本発明の制御トランンザクションのレポート機能の実施例の説明図である。
【図１３】本発明の監視データの転送、及び、その拡張機能の実施例の第１の説明図である。
【図１４】本発明の監視データの転送、及び、その拡張

機能の実施例の第２の説明図である。
【図１５】本発明の監視データの転送、及び、その拡張機能の実施例の第３の説明図である。
【図１６】本発明の監視データの転送、及び、その拡張機能の実施例の第４の説明図である。
【図１７】本発明の監視データの転送、及び、その拡張機能の実施例の第５の説明図である。
【図１８】本発明の監視データの転送、及び、その拡張機能の実施例の第６の説明図である。
【図１９】本発明のメモリアクセスの安全性確保の実施例の第１の説明図である。
【図２０】本発明のメモリアクセスの安全性確保の実施例の第２の説明図である。
【図２１】本発明のアクセスログ、及び、警報機能の実＊施例の第１の説明図である。
【図２２】本発明のアクセスログ、及び、警報機能の実施例の第２の説明図である。
【符号の説明】
１…制御系用ファイウォール（ブラントファイアウォール）、２…情報系ＯＳ（Ｇ－ＯＳ）、３制御系ＲＴ－ＯＳ（ＲＴ－ＯＳ）、１０…共有メモリ、１１…情報系ＬＡＮボード、１２…情報系メモリ・記憶装置、１３…制御系メモリ・記憶装置、１４…制御系ＬＡＮボード、３４…コマンドフィルタリングテーブル、１０００…制御系ＬＡＮ、１００１…監視制御コンピュータ、１００２…制御機器、１００３…計測機器、２０００…情報系ＬＡＮ（イントラネット）、２００１…インターネット、２００４…データベースサーバ、３００１…情報端末。

【図１】

図1



【図３】

図3

動作41	制御コマンド42	送信先43
通過	カメラズーム	カメラ制御装置
遮断	カメラチルト	カメラ制御装置
待機	ポンプ起動	制御コンピュータA
待機	ポンプ停止	制御コンピュータA
遮断	ポンプ保守	制御コンピュータA
通過	ゲート開	制御コンピュータA
通過	ゲート閉	制御コンピュータA

34

【図１１】

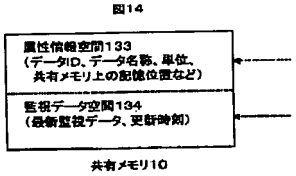
図11

動作41	制御コマンド42	操作権番号104
通過	カメラズーム	R2913
遮断	カメラチルト	R2913
待機	ポンプ起動	－
待機	ポンプ停止	－
遮断	ポンプ保守	－
通過	ゲート開	R315
通過	ゲート閉	R315

34

【図１４】

図14



【図２】

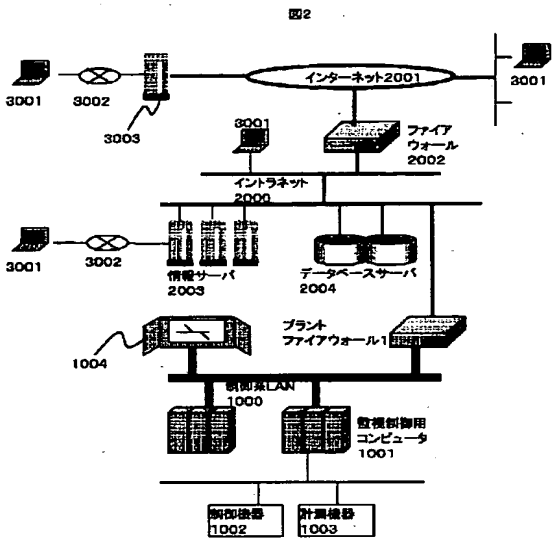


図2
インターネット2001
3001
3002
3003
ファイア
ウォール
2002
イントラネット
2000
情報サーバ
2003
データベースサーバ
2004
プラント
ファイアウォール1
1004
制御系LAN
1000
監視制御用
コンピュータ
1001
制御機器
1002
計測機器
1003

【図４】

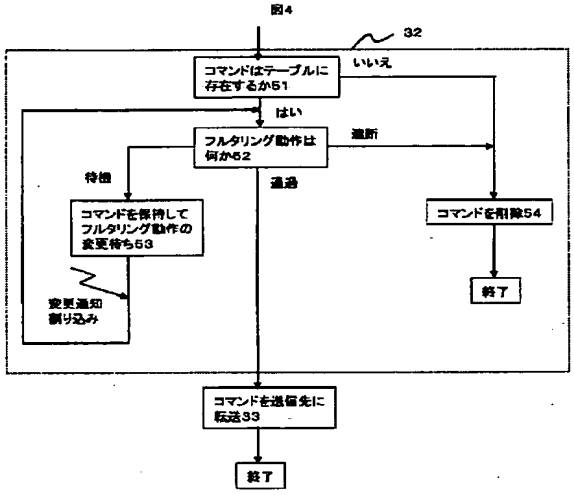


図4
32
コマンドはテーブルに
存在するか51
いいえ
はい
フルタリング動作は
何か52
遮断
待機
通過
コマンドを保持して
フルタリング動作の
変更待ち53
コマンドを削除54
変更通知
割り込み
終了
コマンドを送信先に
転送33
終了

【図５】

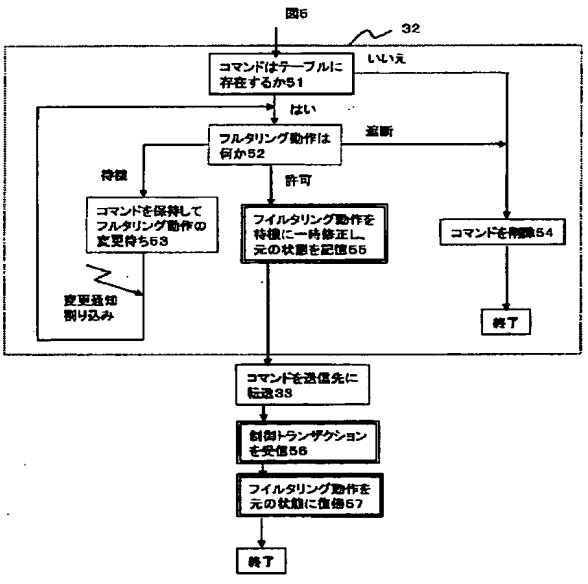


図5
32
コマンドはテーブルに
存在するか51
いいえ
はい
フルタリング動作は
何か52
遮断
待機
許可
コマンドを保持して
フルタリング動作の
変更待ち53
フィルタリング動作を
待機に一時修正し、
元の状態を記憶55
コマンドを削除54
変更通知
割り込み
終了
コマンドを送信先に
転送33
制御トランザクション
を受信56
フィルタリング動作を
元の状態に復帰57
終了

【図６】

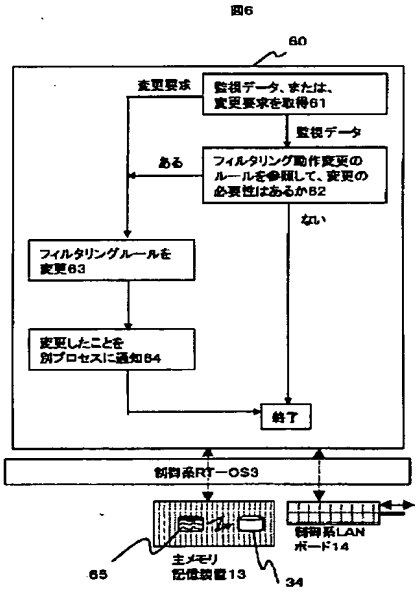
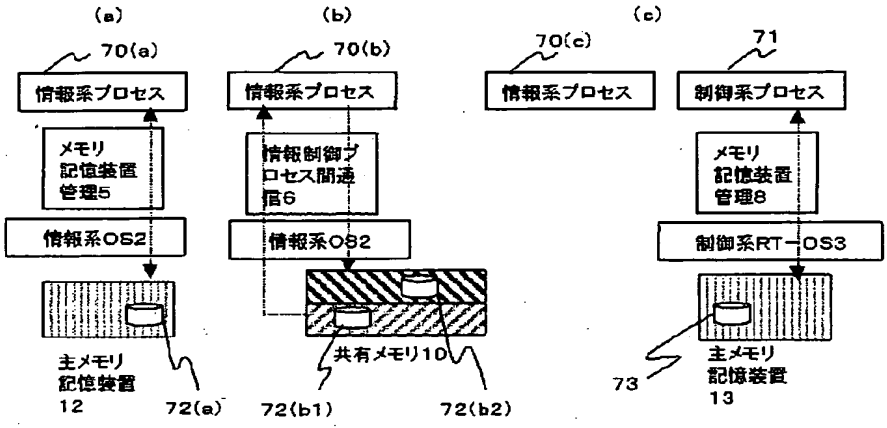


図6
60
変更要求
監視データ、または、
変更要求を取得61
監視データ
ある
フィルタリング動作変更の
ルールを参照して、変更の
必要性はあるか62
ない
フィルタリングルールを
変更63
変更したことを
別プロセスに通知64
終了
制御系RT－OS3
主メモリ
記憶装置13
65
制御系LAN
ボード14
34

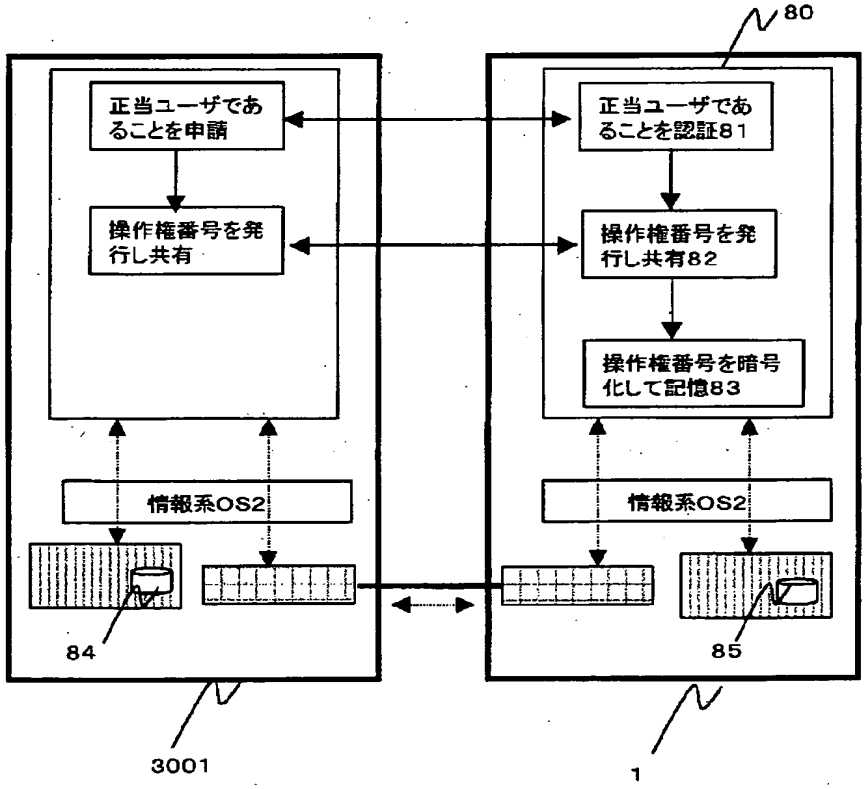
【図７】

図7


(a)
(b)
(c)
70(a)
70(b)
70(c)
71
情報系プロセス
情報系プロセス
情報系プロセス
制御系プロセス
メモリ記憶装置管理5
情報制御プロセス間通信6
メモリ記憶装置管理8
情報系OS2
情報系OS2
制御系RT－OS3
主メモリ記憶装置12
共有メモリ10
主メモリ記憶装置13
72(a)
72(b1)
72(b2)
73

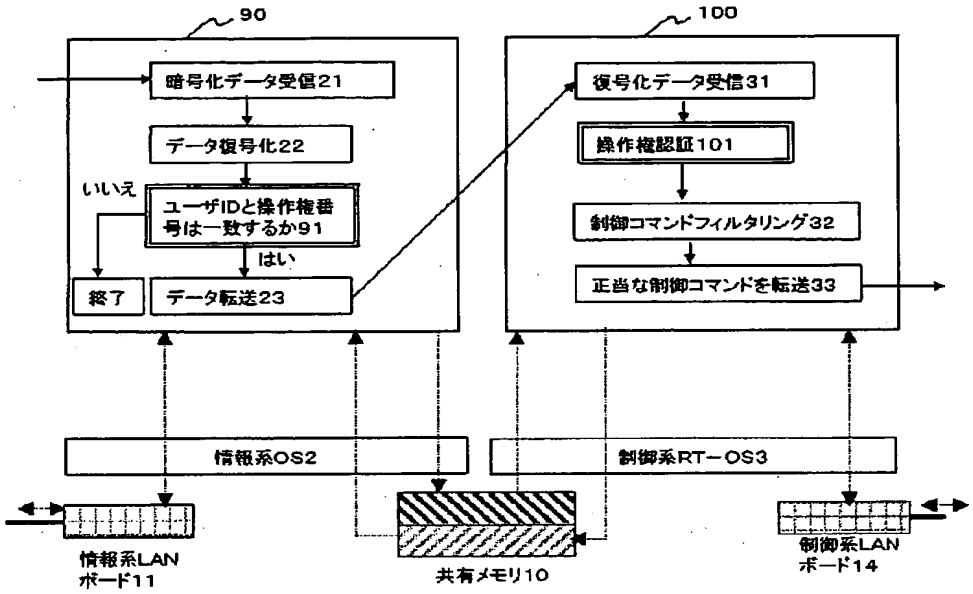
【図８】

図8


80
正当ユーザであることを申請
正当ユーザであることを認証81
操作権番号を発行し共有
操作権番号を発行し共有82
操作権番号を暗号化して記憶83
情報系OS2
情報系OS2
84
85
3001
1

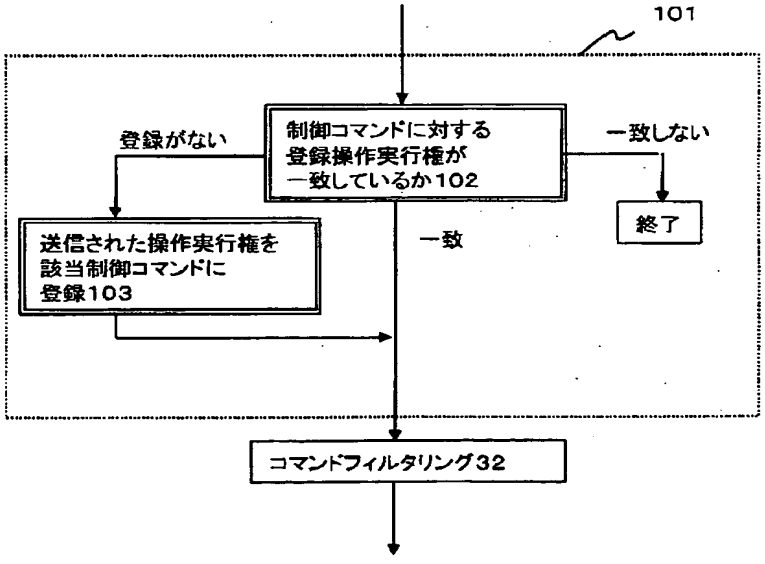
【図９】

図9


90
暗号化データ受信21
データ復号化22
いいえ
ユーザIDと操作権番号は一致するか91
はい
終了
データ転送23
100
復号化データ受信31
操作権認証101
制御コマンドフィルタリング32
正当な制御コマンドを転送33
情報系OS2
制御系RT－OS3
情報系LANボード11
共有メモリ10
制御系LANボード14

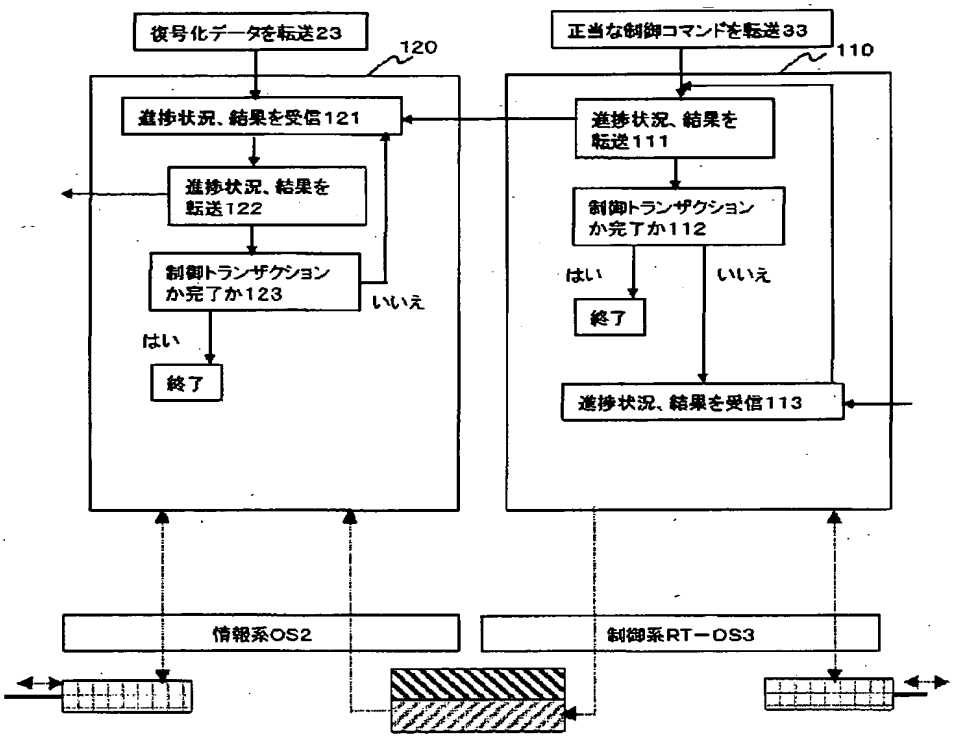
【図１０】

図10


101
制御コマンドに対する登録操作実行権が一致しているか102
登録がない
一致しない
終了
一致
送信された操作実行権を該当制御コマンドに登録103
コマンドフィルタリング32

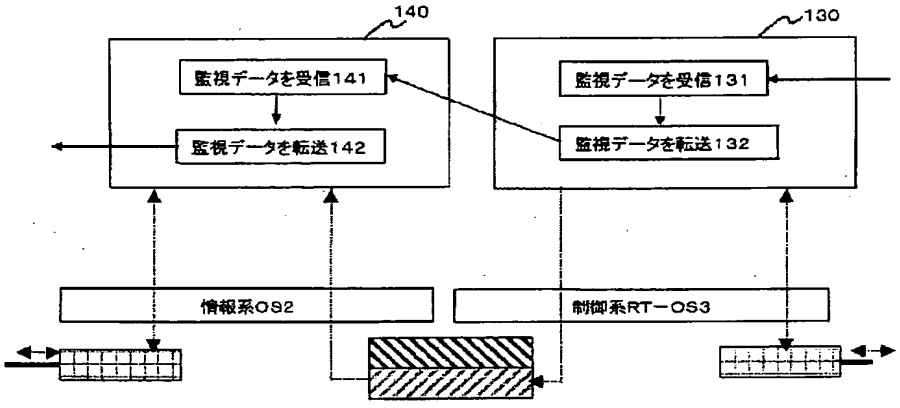
【図１２】

図12



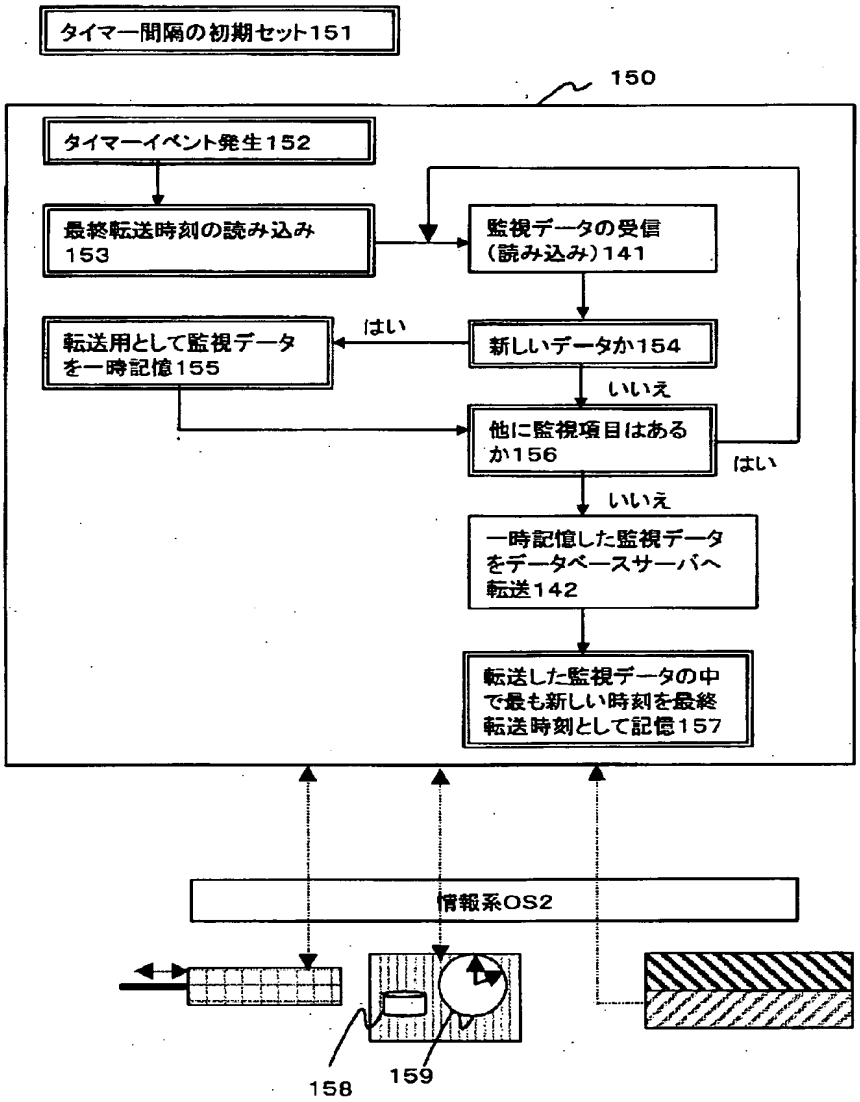
【図１３】

図13



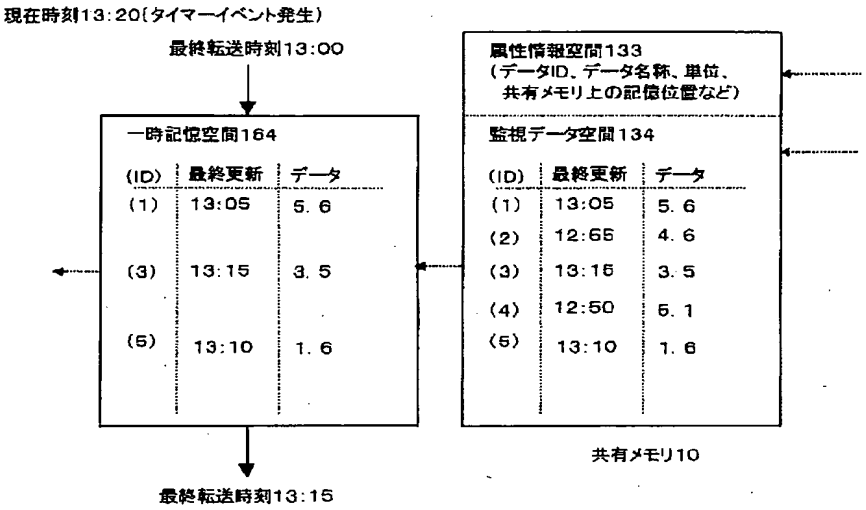
【図１５】

図15

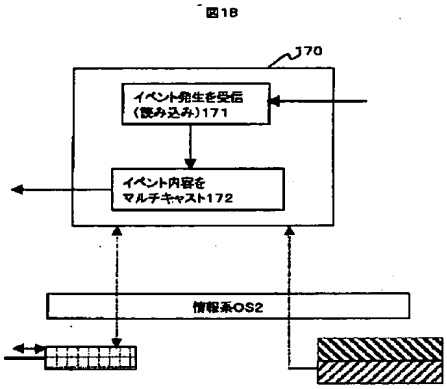

タイマー間隔の初期セット151
150
タイマーイベント発生152
最終転送時刻の読み込み153
監視データの受信（読み込み）141
転送用として監視データを一時記憶155
はい
新しいデータか154
いいえ
他に監視項目はあるか156
はい
いいえ
一時記憶した監視データをデータベースサーバへ転送142
転送した監視データの中で最も新しい時刻を最終転送時刻として記憶157
情報系OS2
158
159

【図１６】

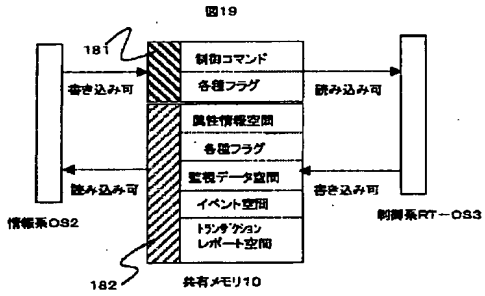
図16



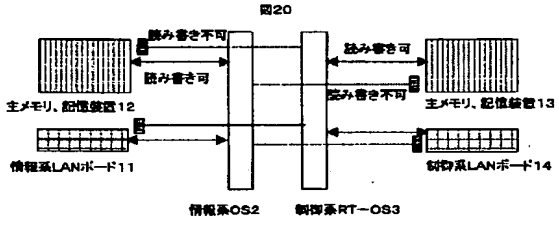
【図１８】



【図１９】

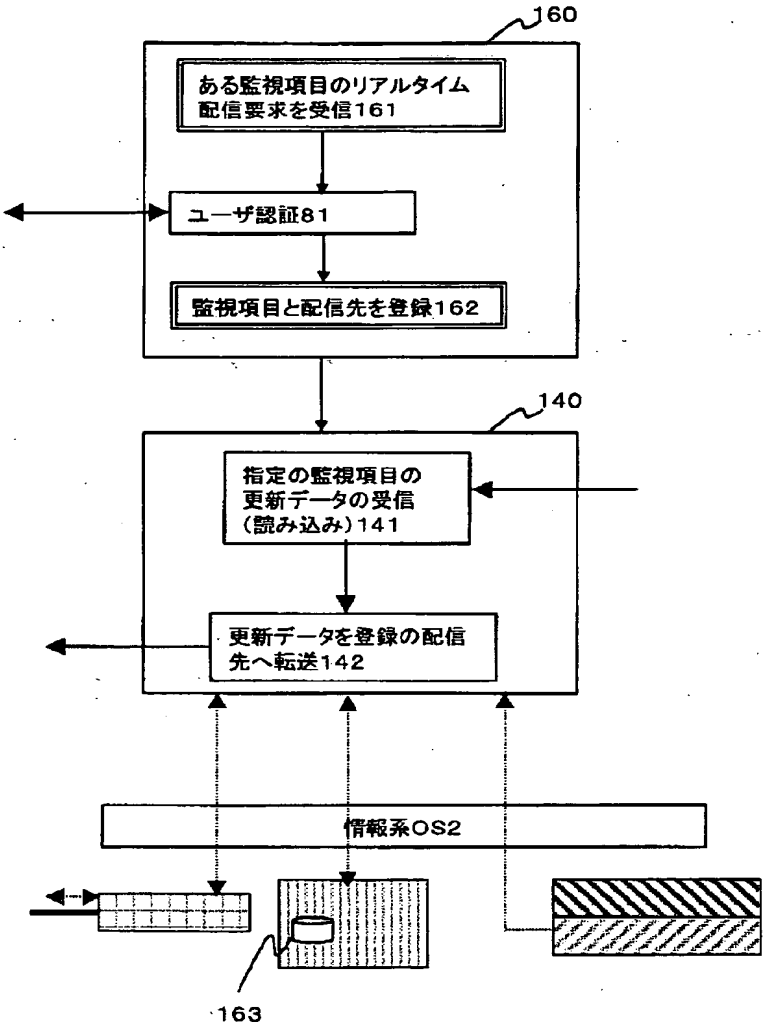


【図２０】



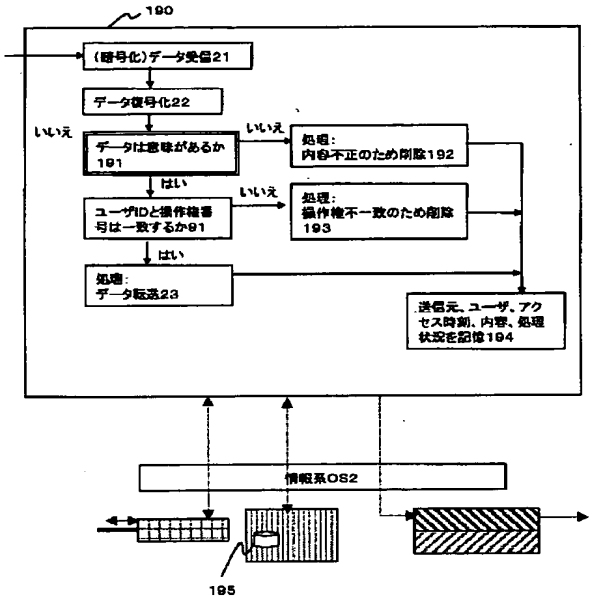
【図１７】

図17


160
ある監視項目のリアルタイム配信要求を受信161
ユーザ認証81
監視項目と配信先を登録162
140
指定の監視項目の更新データの受信（読み込み）141
更新データを登録の配信先へ転送142
情報系OS2
163

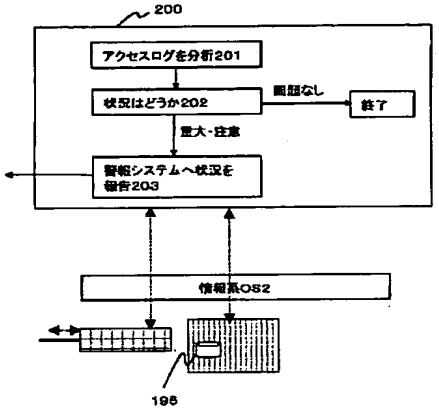
【図２１】

図21



【図２２】

図22



フロントページの続き

(72)発明者　加藤　博光
神奈川県川崎市麻生区王禅寺1099番地　株式会社日立製作所システム開発研究所内

Fターム(参考)　5B089 GA01 GA11 HA06 HA10 JA35
JB10 JB16 KA17 KB04 KB13
KC32 KC53 KC58 KH01
5B098 AA10 GA02 GA04 GC16
5K033 AA08 CB01 CB08 DA01 DA05
DB10 DB12 DB14 DB16 EA07